ABSTRACT

Information Technology and Digital Services Department – "Cyber Security Policy 2.0". – Approved – Orders- Issued.

INFORMATION TECHNOLOGY AND DIGITAL SERVICES (E2) DEPARTMENT

G.O.(Ms) No.21 **Dated: 23.08.2024**

ஸ்ரீ குரோதி, ஆவணி-07

திருவள்ளுவர் ஆண்டு -2055

Read:

1. G.O.(Ms). No. 26, Information Technology(E2), dated 18.09.2020.
2. From the MD, ELCOT, Letter No. ELCOT/IT-Infra/CSA TN/CSP 2.0/2023-24, dated 09.02.2024 enclosing draft "Cyber Security Policy 2.0".

ORDER:

In the Government Order 1st read above, orders were issued for the release of "Tamil Nadu Cyber Security Policy 2020".

2. During the Budget Session 2023-2024, the Hon'ble Minister for Information Technology & Digital Services, among other things, has made the following Announcement on the floor of Tamil Nadu Legislative Assembly on 01.04.2023:-

> "இணையப் பாதுகாப்பு 2.0 (Cyber Security 2.0)
>
> தமிழ்நாடு அரசு 2020-ஆம் ஆண்டில் இணையப் பாதுகாப்புக் கொள்கையை வெளியிட்டது. மாநிலத்தின் தகவல் தொழில்நுட்பச் சொத்துகள் தமிழ்நாடு இணையப் பாதுகாப்புக் கட்டமைப்பால் (CSA-TN) பாதுகாக்கப்படுகின்றன.
>
> மேகக்கணினிய அடிப்படையிலான கம்ப்யூட்டிங், மின்-அலுவலகம் போன்றவற்றின் தற்போதைய போக்கிற்கேற்ப கூடுதலான சொத்துகள் மற்றும் மேம்படுத்தப்பட்ட நடைமுறைகளை உள்ளடக்கிய வகையில் இக்கொள்கை புதுப்பிக்கப்படும்".

3. In the letter 2nd read above, the Managing Director, Electronics Corporation of Tamil Nadu Limited has sent a draft Cyber Security Policy 2.0 after extensive consultation with stakeholders like Centre for Development of Advanced Computing (C-DAC), Indian Institute of Technology Madras (IIT-M) (Pravartak), Tamil Nadu e-Governance Agency and with inputs from other Standard Operating Procedures (SOPs) of National level agencies like CERT-IN for the approval of Government.

..2

4. The Government, after careful examination of the policy have decided to accept and release the "Cyber Security Policy 2.0".

5. Cyber Security Policy 2.0 (CSP 2.0) is applicable to all State Government Departments, State Public Sector Units and other State Government Agencies functioning under Government of Tamil Nadu which uses IT Infrastructure, Network or Digital Data. CSP 2.0 is also applicable to the relevant stakeholders and Third Parties (e.g. Suppliers, Contractors, Consultants and Partners).

6. Some of the salient features of the "Cyber Security Policy 2.0" are as follows:-

- Protect information assets of Government (infrastructure, software, citizen services) and maximize their availability to Government and Citizens.
- Create an institutional mechanism to monitor the established infrastructure.
- Develop a comprehensive security risk reduction strategy.
- Establish security capabilities and infrastructure for layered security of mission-critical systems and data.
- Effective cyber security measures to help in detecting, preventing and mitigating cyber-attacks, thereby minimizing potential damage and losses by establishing protocols / processes, adopting technologies, proactive audits, preventive measures, and drills by ethical hacking.
- Create awareness about basics of cyber security and adoption of cyber security practices among the Government workforce.
- Cooperation and coordination with other cyber security agencies and institutes.
- Issue of guidelines, Standard Operating Procedures (SOP) for audit, compliance and monitoring of cyber threats and attacks.

7. The policy also covers procedures to be adopted on the following:-

- Backup and Recovery
- Critical Assets / Applications
- Securing user endpoints of large-scale/critical applications
- Information Security Audit
- Vulnerability Assessment and Penetration Testing(VAPT)
- Change Management, Incident Management and Problem Management
- e-Sign / Digital Signature Certificate
- e-Mail Security
- Password Policy
- Social Media Policy
- Emerging Technologies
- Capacity Building / Training
- Procedures & Compliances

8. The CSP 2.0 also mandates all departments for the following:-

- Nominating CISOs/ISOs to coordinate with Cyber Security Incident Response Team (CSIRT) to collate information regarding cyber security incidents that take place in Government web sites / applications and IT infrastructure.
- The CISOs and ISOs of all departments shall undergo annual training for one or two days on management of change, incident and problem.
- Every department while hosting application in the Tamil Nadu State Data Centre (TNSDC) or in any other environment shall mandatorily list out the folders, databases and logs that need to be backed up with the periodicity (daily / weekly / monthly / yearly) mentioned.
- The department shall ensure that the backed-up datasets / databases are stored in tapes / external devices or in servers / storage in more than one location – other than the primary space of storage.
- The backed-up datasets shall be restored periodically and confirmed by the department for the correctness and completeness.
- Comprehensive risk assessment to be done by the departments through their CISOs / ISOs to identify and define criticality by evaluating the value, sensitivity, and potential consequences of compromise for each asset / application.
- The departments shall share the list of critical assets / applications with Tamil Nadu-CERT annually. TN-CERT shall carryout random / periodical checks in this regard.
- The departments owning larger / critical applications shall be responsible for carrying out IS audit periodically through CERT–In empanelled vendors. Necessary guidance / support shall be provided by TN-CERT.
- Any application to be hosted in TNSDC or in any other environment under the domain name owned by any department shall mandatorily have the certificate of safe hosting provided by the third-party CERT-In empanelled agencies.
- e-Sign should be made applicable for all the departments delivering citizen centric services by way of issuing certificates and other legal documents.
- e-Mail backups shall be archived and ensured by the department's IT teams.
- Departments shall use the tn.gov.in email account or an email under their registered department / organization domain for all its official communication.
- CISOs / ISOs of the department shall frame the department's guidelines for the e-Mail policy and its usage.
- Departments shall issue guidelines for creating, managing, and protecting passwords to reduce the risk of unauthorized access or data breaches resulting from weak or compromised passwords.
- Departments shall enhance their security posture on social media platforms and reduce the risk of falling victim to cyber threats.

9. A detailed booklet on "Cyber Security Policy 2.0" is annexed to this Order.

10. The Managing Director, Electronics Corporation of Tamil Nadu Limited shall be responsible for the implementation of the Policy with guidance from C-DAC, at the field level and also to monitor the implementation and report the status to the Government periodically.

(By Order of the Governor)

KUMAR JAYANT
ADDITIONAL CHIEF SECRETARY TO GOVERNMENT

To
All Departments of Secretariat, Chennai-600 009.
All Heads of Department, Government of Tamil Nadu.
All District Collectors/ District Magistrates,
All State owned PSUs/Corporations and Statutory Bodies.
The Managing Director,
Electronics Corporation of Tamil Nadu Limited,
II Floor, MHU Complex, 692, Anna Salai, Nandanam, Chennai – 600 035.
The Director of e-Governance and Chief Executive Officer,
Tamil Nadu e-Governance Agency,
No.807, 2nd and 7th Floor, P. T. LEE Chengalvaraya Naicker Building,
Opp. LIC Building, Anna Salai, Chennai – 600 002.
The Registrar, High Court of Madras, Chennai - 600 104.
All HoDs of Information Technology and Digital Services Department.
The Additional Director General of Police,
Cyber Crime Wing, Cyber Crime Division,
O/o. Director General of Police, Mylapore, Chennai – 600 004.
The Director, Centre for Development of Advanced Computing (CDAC),
8th floor, D Block, TIDEL Park, No. 4, SH 49A,Tharamani, Chennai – 600 113.
The Director, Society for Electronic Transactions and Security (SETS),
CIT Campus, Taramani, Chennai - 600 113.
The Director, Standardisation, Testing and Quality Certification (STQC)
Directorate, Thiruvanmiyur, Chennai – 600 041.
The Director (South), NCIIPC, P.B.No.1343, Jalahalli H.P.O,
Bengaluru - 560 013.
The State Informatics Officer, National Informatics Centre, E Wing, First Floor,
Rajaji Bhavan, Besant Nagar, Chennai – 600 090.
The Director of Information and Public Relations, Chennai - 600 009.
The Accountant General, Chennai - 600 018.

Copy to:
O/o. Hon'ble Chief Minister, Secretariat, Chennai- 600 009.
The Special Personal Assistant to Hon'ble Minister for
Information Technology and Digital Services Department, Secretariat,
Chennai- 600 009.
The Principal Private Secretary to Chief Secretary to Government,
Secretariat, Chennai - 600 009.

The Content Creator/ Moderator/ Nodal Officer,
Information Technology and Digital Services Department, Secretariat,
Chennai-600 009.
Sf/Sc.

// Forwarded By Order //

27/8/2024

SECTION OFFICER

27/8/24

Cyber Security Policy 2.0

Table of Contents

1. INTRODUCTION

1.1. Cyber Security is a critical aspect of Governance in today's interconnected digital world. The Governance model of the State and its processes rely increasingly on digital infrastructure for delivering essential public services and therefore securing the transactions and proper maintenance of digital records are critical.

1.2. Protecting Government networks and data from cyber threats is crucial to ensure continuity in Governance and citizen trust. With the rapid expansion of online services, the Government departments in the State are generating and sharing more data than ever before.

1.3. The Government of Tamil Nadu, therefore appreciates the importance of Cyber Security and is focused on adopting all possible measures to deal with cyber threats. A robust Cyber Security policy is essential to guide departments to protect their Information Technology infrastructure from denial of services, theft, financial fraud, privacy breaches, etc.

1.4. Hence, Government of Tamil Nadu has reviewed its existing Cyber Security Policy released in 2020 and hereby releases the revised Cyber Security Policy (CSP 2.0) in alignment with the changing scenarios and the National strategy.

2. SCOPE, MISSION AND OBJECTIVES

Scope

2.1. This Cyber Security Policy 2.0 (CSP 2.0) is broad and is applicable to departments, State Public Sector Units and State Government Agencies functioning under Government of Tamil Nadu and using IT Infrastructure, Network or Digital Data. This CSP 2.0 is also applicable to the relevant stakeholders and Third Parties (e.g. Suppliers, Contractors, Consultants and Partners).

Mission

2.2. To protect the IT infrastructure and application(s) of the Government of Tamil Nadu from cyber-attacks, build capabilities to prevent and respond to cyber threats, create awareness to reduce vulnerabilities and minimize damage from incidents through a combination of institutional mechanism, processes, technology adoption, responsible people and cooperation.

Objectives

2.3. Protect information assets of Government (infrastructure, software, citizen services) and maximize their availability to Government and Citizens.

2.4. Create an institutional mechanism to monitor the established infrastructure.

2.5. Develop a comprehensive security risk reduction strategy.

2.6. Establish security capabilities and infrastructure for layered security of mission-critical systems and data.

2.7. Effective cyber security measures to help in detecting, preventing and mitigating cyber-attacks, thereby minimizing potential damage and losses by establishing protocols / processes, adopting technologies, proactive audits, preventive measures and drills by ethical hacking.

2.8. Create awareness about basics of Cyber Security and adoption of cyber security practices among the Government workforce.

2.9. Cooperation and coordination with other Cyber Security agencies and Institutes.

2.10. Issue of guidelines, Standard Operating Procedures (SOP) for audit, compliance and monitoring of cyber threats and attacks.

3. FOUNDATIONAL PRINCIPLES

3.1. Confidentiality - Only authorized individuals or systems shall access sensitive data. Techniques such as encryption, access controls, data masking & anonymization, secure communication protocols and data classification & handling are to be used to protect confidentiality.

3.2. Integrity - Data should remain accurate, consistent, intact, uncorrupted and trustworthy throughout its lifecycle. The key strategies such as data encryption, access controls, data validation, hash functions, change management and digital signatures should be used to maintain the integrity and to prevent unauthorized alterations.

3.3. Availability - Availability of systems and data to authorized users shall be ensured by mitigating service disruptions caused by cyber attacks or technical failures. The key aspects are preventing downtime, resilience, redundancy and Standard Operating Procedure (SOP) based incident response.

4. TAMIL NADU CERT (TN-CERT)

4.1. Information Technology & Digital Services Department, Government of Tamil Nadu provides support for all IT and e-Governance initiatives in the State through its constituent organizations viz., Directorate of

e-Governance (DeG) which will act as a regulator and standard setting agency, Electronics Corporation of Tamil Nadu Limited (ELCOT) (Procurement and IT Infrastructure support), Tamil Nadu e-Governance Agency (TNeGA) (IT application development, consultancy and security support), Tamil Nadu FibreNet Corporation Limited (TANFINET) (network / connectivity support), i –Tamil Nadu Technology Hub (ecosystems for startups and industries towards innovation), ICT Academy (capacity building by training, support in research & development).

4.2. In line with the CERT-In, the National nodal agency for responding to computer security incidents, Government of Tamil Nadu hereby establishes the Tamil Nadu - Computer Emergency Response Team (TN-CERT) under the Directorate of e-Governance, IT&DS Department, Government of Tamil Nadu.

4.3. TN-CERT shall function as an autonomous body and coordinate with all the departments in the Government of Tamil Nadu.

4.4. TN-CERT shall be primarily responsible for the effective implementation of Cyber Security Policy in collaboration with all Heads of the Departments under IT&DS Department.

4.5. TN-CERT will collaborate primarily with ELCOT, TNeGA and TANFINET for addressing Cyber Security issues related with IT Infrastructure, application development and network connectivity.

4.6.TN-CERT shall also be responsible for the following:

- Performing independent audit of various applications for vulnerabilities identification.
- Provide technical advisory and support to system administrators/ development team and users to respond, manage and mitigate the Cyber Security incidents.
- Identify trends in intruder activities and analyze the same for mitigation.
- Collaborate with other similar institutions & organizations to resolve major security issues.
- Dissemination of information related to incidents and vulnerabilities to concerned stakeholders.
- Issues guidelines, Standard Operating Procedures (SOP), advisories and white-papers related to Cyber Security events.
- Coordinate with all departments in identifying the Chief Information Security Officers (CISOs) and Information Security Officers (ISOs).
- Provide periodical training to CISOs and ISOs on Cyber Security.
- Conduct annual evaluation on implementation of Cyber Security policy and;
- Any other functions related to Cyber Security.

4.7. The Cyber Security Architecture for Tamil Nadu (CSA-TN) team already established under ELCOT in accordance with G.O. (D) No. 24, IT (B4) Department dated 01.11.2018 shall be transferred in to DeG and shall function under the name of TN-CERT with the following divisions:

1. Cyber Security Incident Response Team (CSIRT)

a) To collate information regarding Cyber Security incidents that take place in Government web sites / applications and IT infrastructure.

b) To coordinate with the trusted Government entities / agencies i.e., Indian Computer Emergency Response Team (CERT-In), National Informatics Centre Computer Emergency Response Team (NIC CERT), National Critical Information Infrastructure Protection Centre (NCIIPC), Subsidiary Intelligence Bureaus (SIB), Cyber Crime Cell.

c) To communicate the CISOs / ISOs of departments about the incident and issue suitable directions/advisories for closure of incidents.

d) To follow-up with the CISOs / ISOs of departments on closure of incidents and send a detailed report to Government of Tamil Nadu (GoTN) and other stake-holders as may be required.

e) To communicate vulnerabilities reported by various trusted agencies to the concerned departments.

f) To follow-up with the departments on closing of vulnerabilities and send a detailed report to Government of Tamil Nadu and other stake-holders as required.

g) To issue guidelines, advisories, vulnerability notes and whitepapers on security practices, procedures, prevention and response for Cyber Security issues.

h) To conduct awareness and training program for the Officials of Government of Tamil Nadu.

2. Security Operation Centre (SOC):

a) To perform vulnerability assessment of all Government applications.

b) To provide solution document / guidance to departments for identified vulnerabilities.

c) To monitor all Government applications for intrusions / incidents through various Cyber Security tools and raise suitable alert.

d) To provide mitigation measures on cyber incidents / intrusions for affected systems.

e) To conduct mock drill periodically for the applications of departments of Government of Tamil Nadu.

3. Cyber Crisis Management Plan (CCMP):

a) Cyber Crisis Management Plan (CCMP) is a strategic framework to prepare for, respond to and initiate recovery from a cyber-incident in accordance with National efforts for countering cyber-attacks and cyber terrorism.

b) CCMP process shall be technically / administratively carried out through CSIRT of TN-CERT.

5. COMPONENTS & PRACTICES

5.1. Cyber security is an ongoing process that requires continuous monitoring, adaptation to new threats and proactive measures to protect critical assets. The following key components and practices are to be adopted in all departmental applications and hosting infrastructure on priority:

a. Network Security
b. Application Security
c. Database Security
d. Operating System Security
e. Server monitoring
f. Endpoint Security
g. Vulnerability Assessment and Penetration Testing (VAPT)
h. Identity and Access Management (IAM)
i. Incident Response
j. Services of Security Operations Center (SOC)
k. Cloud Security.

6. BACKUP AND RECOVERY

6.1. Every department while hosting application in the Tamil Nadu State Data Centre (TNSDC) or in any other environment shall mandatorily list out the folders, databases and logs that need to be backed up with the periodicity (daily / weekly / monthly / yearly) mentioned.

6.2. The department shall ensure that the backed-up datasets / databases are stored in tapes / external devices or in servers / storage in more than one location – other than the primary space of storage.

6.3. The backed-up datasets shall be restored periodically and confirmed by the department for the correctness and completeness.

6.4. TN-CERT shall conduct a random audit of Government applications for backup and recovery process.

7. CRITICAL ASSETS / APPLICATIONS

7.1. Critical assets are the specific resources which are most vital for financial systems, healthcare systems, emergency services systems, fire service, transportation, utility services and telecommunications which have the highest impact in the event of security breach.

7.2. Critical assets / applications include data, systems, networks, physical infrastructure, people and third-party contracts (vendors, developers, system integrators and other partners).

7.3. Comprehensive risk assessment to be done by the departments through their CISOs / ISOs to identify and define criticality by evaluating the value, sensitivity, and potential consequences of compromise for each asset / application. Necessary guidance will be provided by TN- CERT.

7.4. The department/ System Integrator shall employ the strategies like secure architecture design, authentication and authorization, data encryption, Secure Development Life Cycle (SDLC), patch management, monitoring and logging, host intrusion detection and prevention, incident response plan, security awareness and training, third-party risk management, compliance and regulations and continuous improvement.

7.5. The departments / System Integrators of critical assets / applications shall comply to the standards / processes established by TN-CERT.

7.6. The departments shall share the list of critical assets/ applications with TN-CERT annually. TN-CERT shall carryout random / periodical checks in this regard.

7.7. TN-CERT shall also access the critical assets / applications through its internal ethical hacking team to ensure the stability and security of the system.

7.8. TN-CERT shall carry out regular Information Security (IS) Audit & Penetration Testing for mitigating Cyber Security incidents. The observations reported shall be immediately addressed by the concerned owners.

7.9. In the event of any major threat / vulnerability identified on these critical assets / applications and if not resolved within a reasonable time, TN-CERT is empowered to shut down or take-out the application from the network until, resolved.

8. SECURING USER ENDPOINTS OF LARGE-SCALE / CRITICAL APPLICATIONS

8.1. The user end points like Desktop, Laptop, Point of Sale (PoS) Mobile devices etc., are to be protected on par with Servers.

8.2. The departments shall be responsible for establishing the layered defense approach as detailed below. Necessary support / guidance shall be provided by TN-CERT.

- **Network Isolation:** Limits the scope of attacks and prevents lateral movement within the network.
- **Separate Domain Tree:** Provides a distinct security boundary for user accounts and resources, reducing the impact of credential theft or compromise.
- **Antivirus Management:** Ensures all endpoints have up-to-date antivirus protection and enables centralized monitoring and response to threats.
- **Patch Management:** Minimizes vulnerabilities by keeping software and systems patched and updated against known security issues.

9. INFORMATION SECURITY AUDIT

9.1. An Information Security (IS) audit is a systematic evaluation to ensure the compliance with established security standards, policies & procedures, regulations and best practices. The primary goal of an Information Security audit is to assess the effectiveness of existing security controls and recommend for improvements.

9.2. The departments owning larger / critical applications shall be responsible for carrying out IS audit periodically through CERT–In empaneled vendors. Necessary guidance / support shall be provided by TN-CERT.

9.3. Failing to conduct regular IS audit can have serious consequences for departments such as data breaches, financial loss, etc. The department will be held responsible to comply with IS audit.

10. VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT)

10.1. VAPT plays a critical role in helping departments to assess, manage and mitigate Cyber Security risks effectively, thereby strengthening overall security posture and resilience against evolving cyber threats.

10.2. VAPT shall be performed by CERT-In empaneled agencies for all applications once in a year or every time the major change / update is done in the application.

10.3. Any application to be hosted in TNSDC or in any other environment under the domain name owned by any department shall mandatorily have the certificate of safe hosting provided by the third-party CERT-In empaneled agencies.

10.4. The Government of Tamil Nadu shall fund for security audit through IT&DS Department to TN-CERT.

10.5. TN-CERT shall regularly monitor and identify the applications hosted in TNSDC or any other environment for validity of safe hosting certificate.

10.6. The reported vulnerability shall be promptly handled by the appropriate level of expertise for receipt, ticketing, triage, analysis and develop containment or response plan and shall be fixed within the time line indicated in the SOP released by TN-CERT time to time.

10.7. TN-CERT shall be empowered to shut down or take action to remove such applications from the network in case of non-compliance.

11. CHANGE MANAGEMENT, INCIDENT MANAGEMENT AND PROBLEM MANAGEMENT

11.1. Change management is a structured process used to ensure that changes to information systems, networks and applications are carried out in a controlled and coordinated manner so as to minimize risks, ensure security and maintain the integrity of the systems.

11.2. Incident management is a systematic process of detecting, responding to, and recovering from Cyber Security incidents. This process is essential to protect Department's information assets and minimize the impact of security breaches.

11.3. Problem management refers to the structured approach of identifying, analyzing and resolving underlying issues that cause incidents and security breaches. It aims to prevent recurring problems and minimize the impact of incidents that cannot be prevented.

11.4. The Departments handling larger /critical applications shall implement the above measures failing which will make impact on data loss and business continuity.

11.5. In case of reporting of an incident, TN-CERT shall do the triaging. On confirmation of incident, action will be taken by TN-CERT as per SOP in coordination with departments for resolution.

11.6. The CISOs and ISOs of all Departments shall undergo annual training for one or two days on management of change, incident and problem.

12. e-SIGN / DIGITAL SIGNATURE CERTIFICATE (DSC)

12.1. Electronic Signature (e-Sign): An electronic signature is an electronic symbol, logically associated with a document with the intent to sign the document. e-Sign plays a major role in enhancing the security, integrity, and authenticity of digital communications and transactions.

12.2. e-Sign shall be applicable for all the departments delivering citizen centric services by way of issuing certificates and other legal documents.

12.3. e-Sign shall be provided to all approving authorities in the departments which are delivering citizen centric services to authenticate the documents issued to the citizens and to approve the files moved through e-Office / ERP.

12.4. The departments which are currently using DSC devices shall mandate the users to register and promote the use of e-sign for all its certification and approval process.

12.5. DeG / TNeGA / ELCOT shall provide infrastructure and IT/security systems for e-Sign implementation and its verification process.

12.6. User training shall be provided for the implementation of e-Sign by TN-CERT. transfer of officers and thereby the process of transfer and role changes in the applications towards security of implementation shall be managed by the respective departments.

13. e-MAIL SECURITY

13.1. Given the critical role of e-mail in official communications ensuring its security is vital to prevent threats such as phishing, malware, spam, and unauthorized access.

13.2. Prevention Strategies: e-Mail Filtering and Anti-Malware Software, Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC) Protocols, e-mail Encryption, user authentication and regular software updates.

13.3. Mitigation Strategies: User awareness training, incident response plan, e-mail usage policies, monitoring and alerts, Data Loss Prevention (DLP) and backup & recovery.

13.4. Additional Recommendations: Security audits, use of secure e-mail services, employee empowerment and collaboration with third-party services.

13.5. e-Mail backups shall be archived and ensured by the department's IT teams.

13.6. Departments shall use the tn.gov.in email account or an email under their registered department / organization domain for all its official communication.

13.7. Users should be aware of phishing attempts through e-Mail and spam filters to be used to detect and filter out the same.

13.8. Clicking on links or downloading attachments from unknown or suspicious emails shall be avoided.

13.9. TN-CERT will issue the SOP on e-Mail security periodically. CISOs / ISOs of the department shall frame the department's guidelines for the e-Mail policy and its usage.

14. PASSWORD POLICY

14.1. To reduce the risk of unauthorized access or data breaches resulting from weak or compromised passwords, departments shall issue guidelines for creating, managing, and protecting passwords.

14.2. Complex passwords using a combination of uppercase & lowercase letters, numbers and special characters shall be used.

14.3. A minimum length for passwords shall be specified to resist attacks. Longer passwords are generally more secure.

14.4. After a certain number of failed login attempts, user account should be temporarily locked to prevent unauthorized access.

14.5. Two-Factor Authentication (TFA) or Multi-Factor Authentication (MFA) shall be adopted for accessing sensitive systems or resources.

14.6. To reduce the risk of compromise, passwords must be changed periodically.

14.7. Procedures to be established for securely resetting or recovering passwords in the event of users forgetting the passwords. This may involve verifying user's identity through alternate means, such as security questions or biometric authentication.

14.8. Regular monitoring for compliance with the password policy and enforcement of account lockouts or disciplinary actions for violations shall be followed.

15. SOCIAL MEDIA POLICY

15.1. Departments shall enhance their security posture on social media platforms and reduce the risk of falling victim to cyber threats.

15.2. Unique, complex passwords and enablement of Multi-Factor Authentication (MFA) shall be enabled for each social media account.

15.3. Regular review and adjustment of privacy settings to be done and visibility of profile to be limited only to trusted connections.

15.4. Users should be vigilant on phishing attempts via social media messages, posts and links.

15.5. Account recovery options such as alternative e-mail addresses or phone numbers shall be enabled to regain access to the account and these recovery methods are to be kept secure and up to date.

16. EMERGING TECHNOLOGIES

16.1. The use of Emerging technologies in Cyber Security are spurring innovations and advancements and will become necessary to address new and evolving threats.

16.2. Tools using AI and Machine Learning, Zero Trust Architecture, Secure Access Service Edge (SASE), Block chain for security, homomorphic encryption, threat intelligence platforms, deception technologies, IoT security solutions, behavioral biometrics and container security will be adopted under the policy for countering sophisticated cyber-attacks.

16.3. TN-CERT shall continuously engage with research agencies / other institutes of eminence in these related areas towards adopting them for securing the IT infrastructure and applications of Government departments.

17. CAPACITY BUILDING / TRAINING

17.1. Assessing the specific needs within departments and identifying the areas where knowledge and skill gaps exist is an important activity which will be done by TN-CERT, annually.

17.2. As part of its annual assessment, it shall perform the following:

- Establishing clear training objectives, i.e., specific, measurable, achievable, relevant, and time-bound.
- Designing a comprehensive curriculum tailored to the identified needs and objectives.
- Choosing appropriate training methods based on the target audience, available resources, and learning preferences (in-person workshops / online courses / hands-on exercises / self-paced learning modules, etc.).
- Continuously assessing the effectiveness of the training program. Soliciting input from participants to identify areas for improvement and future training needs.

17.3. TN-CERT shall offer regular training sessions, update materials to reflect the latest threats and best practices and promote a culture of Cyber Security awareness.

17.4. Building a robust Cyber Security training program that empowers individuals and organizations to better protect themselves against cyber threats shall be a mandate for TN-CERT.

17.5. The departments are encouraged to send the CISO / ISO and other technical team members for certifications or recognition in training programs given by Third party agencies. These shall act as motivation for individuals to engage fully with the material and demonstrate their expertise in Cyber Security.

18. PROCEDURES AND COMPLIANCES

TN-CERT shall perform its supervisory and independent audit function ensuring that the policies / framework spelt in this Cyber Security Policy 2.0 is complied with its true spirit. Following procedures and compliances shall be adopted by TN-CERT and departments in all its applications:

18.1. Clear and comprehensive Cyber Security procedures tailored to department's internal needs must be developed.

18.2. A detailed incident response plan outlining the steps to be taken in the event of a Cyber Security breach or incident will be developed.

18.3. Adherence by the vendors (system providers / application developers) to Cyber Security best practices and robust security measures by way of Service Level Agreement (SLA) etc. should be ensured.

18.4. Compliance with SSL (Secure Sockets Layer) while hosting and maintaining the application / website at Tamil Nadu State Date Centre (TNSDC) should be ensured.

18.5. Use of wildcard SSL certificate will be promoted for convenient and cost-effective solution for securing multiple sub domains under a single domain with a simplified management, flexibility, scalability and uniform security etc.

18.6. Compliance with VAPT will be mandatory to host and maintain the application / website at Tamil Nadu State Date Centre (TNSDC).

18.7. Software stack (operating system /middleware / database) to stable version (or) N-1 / N- 2 version for the compliance of hosting at TNSDC is mandatory and no beta or testing versions allowed in production environment.

18.8. All applications / websites shall be enabled with Annual Technical Support (ATS) at any point of time and security patches to be applied on time released by respective OEM.

18.9. Adaptation of open standards and data sharing for fostering collaboration, interoperability and improved security practices on threat intelligence sharing, common vulnerability reporting, data

protection & privacy, regulatory compliance & auditing, innovation & collaboration and reduced vendor lock-in etc. will be promoted.

18.10. TN-CERT shall develop & release implementation guidelines for Cyber Security Policy 2.0 (CSP 2.0).

18.11. TN - CERT shall develop and release Standard Operating Procedure (SOP) from time to time for the reference of departments for handling Cyber Security issues, closure of vulnerabilities reported and incidents faced.

18.12. TN-CERT shall be established as a Centre of Excellence (CoE) for Cyber Security, Cyber forensic and regularity framework for the State.

18.13. All Secretariat departments and their respective Heads of the Department (HoDs) shall nominate Chief Information Security Officers (CISOs) and Information Security Officers (ISOs) for effective management of Cyber Security issues.

18.14. Open-source software to be adopted based on the need of transparency, rapid bug fixes, independence from a single vendor, peer review, community support, flexibility, customization and software stack.

18.15. The Cyber Security procedures shall align with relevant compliance standards and regulations such as National Institute of Standards and Technology (NIST) Framework, General Data Protection Regulation (GDPR) and Payment Card Industry Data Security Standard (PCIDSS) etc.

18.16. Personal data stored in databases shall be encrypted to protect sensitive information.

18.17. Adherence to The Digital Personal Data Protection Act (DPDPA), 2023, shall be ensured.

18.18. Department shall ensure the secure usage of wireless networks.

18.19. Cloud storage security shall be maintained with data encryption, robust access controls, Data Loss Prevention (DLP) solution etc.

18.20. Cloud computing security shall be maintained with secure APIs, implementing identity and access management (IAM) solutions etc.

18.21. Storage security policies shall be developed and used with data classification, Role-Based Access Control (RBAC), data-at-rest encryption and data integrity.

18.22. Comprehensive Cyber Security policy to be adopted when considering applications for cloud computing.

18.23. Security features shall be adopted for software coding such as input validation, authentication and authorization, session management etc.

18.24. Encryption of data during Application Programming Interface (API) calls for protecting personal and payment-related information shall be implemented.

18.25. Data sharing across systems for various purposes, including collaboration, analysis, and efficiency shall be done in secured manner.

18.26. Protection of sensitive financial information is mandatory. Key standards like PCIDSS (Payment Card Industry Data Security Standard) to be adopted for secure operation of payment transactions.

18.27. The departments to refer the Reference Standards released by Government of Tamil Nadu for various IT domains including Cyber Security, Interoperability, etc. vide G.O.(Ms.) No. 3, Information Technology (E2) Department. dated 20.01.2022.

KUMAR JAYANT
ADDITIONAL CHIEF SECRETARY TO GOVERNMENT

// True Copy //

27/8/2024
SECTION OFFICER

27/8/24